CareData Application Service Provider Privacy & Security Policies

Access	Discretionary Access Control (DAC) is the security attribute that enforces "need to know" for users of the CAREDATA. It defines and controls access between named users and objects. Objects within the CAREDATA represent data elements that represent healthcare and demographic data related to patients. For purposes of privacy, access controls must be provided to prevent unauthorized access to data. To perform this function the CAREDATA implements DAC through the CAREDATA Application and the returned security keys from CAREDATA to govern access into the data elements.
Authorization	CAREDATA will provide C2-level security functionality in a multi-user environment. System users can authorize or restrict access to data elements or records within their area of responsibility. This is accomplished by means of a Discretionary Access Control (DAC) policy, which is enforced through the CAREDATA Security subsystem. However, it must be understood that the effectiveness of these system security mechanisms is dependent upon their employment by the System Administrator. The CAREDATA Security subsystem provides a single system through which all access to objects, including files on disk, processes in memory, or ports to external devices are checked so that no application or user gets access without proper authorization.
Authentication	Identification and Authentication mechanisms provide the system with the ability to identify by user name (identification) the individual attempting to access the system and the proof of identification (authentication) through use of a password unique to that individual. Associated with that user name are the rights and permissions to access the system, its files and/or data elements. The I&A procedures of a system are critical to the correct operation of all other TCB security features. If I & A is successfully circumvented, then all audited actions become unreliable, because an incorrect user name could be associated with auditable actions. The identification & authentication system implemented by CAREDATA is a typical *UserID* (user name) and password combination. This combination is maintained along with the security token in the CAREDATA host system. The CAREDATA Application enforces either through CAREDATA policies and procedures or through review all the following CAREDATA username and password characteristics. Before being allowed to access the system, each user must identify themselves by entering a unique *UserID* and password. The system uses this data to validate a user's right to access the system. If the credentials are valid, the user is granted a security token, which is used to validate any object access during that particular logon session. Furthermore, the user's logon information can be used to track actions performed by the user. CAREDATA passwords are set and administered by administrators. CAREDATA requires that each user have a valid CAREDATA access and verify code. Current CAREDATA password requirements are that each password shall have no less than eight characters and no more than 20 alphanumeric characters. Each password must contain at least one number. Each password has a maximum lifetime of 120 days. When a password is expired the system will prompt the user has to contact the System Administrator to change it. Any user is locked out after three failed attempts (Configurable) to login.

	CAREDATA system users are instructed to lock his/her workstation upon leaving the console for a short period of time. The system automatically locks after 15 inactive minutes, which forces the user to login upon returning to the system. CAREDATA users are also instructed to safeguard passwords, to never post or write down passwords but instead to commit them to memory. Users are also encouraged to not use passwords of an obvious or personal nature. For access to CAREDATA servers by database or system administrators, the password management mechanism for CAREDATA enforces strong password functionality. CAREDATA designates password-related account policy through the User Manager. Refer to Setting the Account Policy for Passwords in Section 4 for procedures on setting the I&A parameters. Changes made to the account policy are global in that they affect all users of the computer or domain. **Password Screening**: CAREDATA supports moderate password screening. CAREDATA verifies that the new password is minimum of 8 characters in length (see Minimum Password Length below) and must contain at least one Numeric character **Minimum Password Length**: Sets the minimum allowable length of user entered passwords. This is a critical setting since short passwords are easier to crack by a hacker. For CAREDATA this will be set to eight (8) characters. **Password Aging:** The system maintains the following for the password. **Minimum Password Age.** By default, CAREDATA allows users to change their passwords repeatedly immediately following one another. This allows them to change their password when prompted by the system. For CAREDATA the minimal password notification period is 30 days (Configurable). **Maximum Password Age.** This is the period of time that a user is allowed to use a password before the system requires the user to change their password. If the password is not changed prior to this date, the system will not allow the user to login and the user has to contact the System Administrator. For CAREDATA the maximum password notification period is 120 days (Configurable).
Audit	Auditing is handled by the CAREDATA Application and stored in the Microsoft SQL Server 2005 database in the Audit Log schema. All data requests are processed by functions in the CAREDATA Application, which performs the auditing function storing the relevant logs in the CAREDATA database. Review of these Audit Log records are allowed only for System Administrator. CAREDATA System Administrators will be responsible for maintenance of the security in CAREDATA. CAREDATA SA's shall maintain the required level of security clearance appropriate to maintain health care related data.
Secondary Uses of Data	Application handles two categories of data ❖ Read-only Reference data ❖ Transient data **Read only reference Data** Read-only reference data is the data used by the client for reference purposes only. Any sort of DML operations like insert, update delete are restricted. The uses of reference data includes

	1. Providing a static reference or look up data such as patient list, follow-up list etc which will be presented to the user with search, print and export functionalities wherever applicable. 2. Supporting data validation for checking the correctness of user entry **Transient Data** Transient data is the data that can be changed by the user that actually updates the original data on the server. Data can be changed through Insertion, updates or deletion as a direct or indirect result of user input and manipulation. All important database activities will be identified and audit trail will be maintained to track the history of data modifications that have happened in the server.
Data Ownership	Microsoft SQL Server 2005 database system can be quite large and have many users. Someone or some group of people must manage this system. The database administrator (DBA) is this manager. Every database requires at least one person to perform administrative duties. For the CAREDATA system, the DBAs may be located at the Program office and administer the system remotely or be located at the MTF's. DBA's are responsible for: (1) Installing and upgrading the Microsoft SQL Server 2005 Server and application tools. (2) Allocating system storage and planning future storage requirements for the database system. (3) creating primary database storage structures (tablespaces) (4) creating primary objects (tables, views, indexes) (5) modifying the database structure, as necessary, from information given by CAREDATA Program Office (SCRs, product updates, bug fixes) (6) Enrolling users and maintaining system security. (7) Controlling and monitoring user access to the database. (8) Monitoring and optimizing the performance of the database. (9) Planning for backup and recovery of CAREDATA database information. (10) Backing up and restoring the database. (11) Contacting Microsoft SQL Server 2005 Corporation for technical support. Each MTF will have one or more CAREDATA administrators who will have limited day-to-day operation responsibility for their MTF's database. Responsibilities such as controlling and monitoring user access to the database, monitoring the performance of the database, planning for backup and recovery of database information, and backing up and restoring the database will be accomplished by the database or system administrators at the MTF. **Security Officers** In some cases, an MTF may have one or more security officers responsible controlling and monitoring user access to the database, and maintaining system security.